

## **CLAIMS**

What is claimed is:

1. A computer-implemented method comprising:  
encrypting a copy of at least one part of content having a first watermark;  
encrypting a copy of at least one part of the content having a second watermark;  
and  
combining parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.
2. The computer-implemented method of claim 1, wherein the first watermark includes "0s" and the second watermark includes "1s."
3. The computer-implemented method of claim 1, further comprising:  
distributing the combined parts to one or more clients on a network.
4. The computer-implemented method of claim 3, wherein the network includes an Internet network.
5. The computer-implemented method of claim 1, further comprising:  
encrypting a neutral part of the content; and  
combining parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

6. A server comprising:
- a storage device to store content; and
- an encryption module to encrypt a copy of at least one part of the content having a first watermark, to encrypt a copy of at least one part of the content having a second watermark, and to combine parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.
7. The server of claim 6, wherein the first watermark includes "0s" and the second watermark includes "1s."
8. The server of claim 6, wherein the server is to distribute the combined parts to one or more clients on a network.
9. The server of claim 6, wherein the network includes an Internet network.
10. The server of claim 6, wherein the encryption module is to encrypt a neutral part of the content and to combine parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

11. A computing system comprising:  
means for storing content; and  
means for encrypting a copy of at least one part of the content having a first watermark, a copy of at least one part of the content having a second watermark; and  
means for combining parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.
12. The computing system of claim 11, wherein the first watermark includes "0s" and the second watermark includes "1s."
13. The computing system of claim 11, further comprising:  
means for distributing the combined parts to one or more clients on a network.
14. The computing system of claim 13, wherein the network includes an Internet network.
15. The computing system of claim 11, further comprising:  
means for scrambling a neutral part of the content; and  
means for combining parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

16. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:

encrypting a copy of at least one part of content having a first watermark;

encrypting a copy of at least one part of the content having a second watermark;

and

combining parts of the scrambled copy with the first watermark and parts of the scrambled copy with the second watermark in a manner unique for an individual client.

17. A digital processing system comprising:

a storage device to store an encrypted copy of at least one part of content watermarked with a first identifier and an encrypted copy of at least one part of the content watermarked with a second identifier; and

a processing unit coupled to the storage device, the processing unit to combine parts of the encrypted copy watermarked with the first and second identifiers unique to an individual client.

18. The digital processing system of claim 17, wherein the processing unit is to send the combined parts to the individual client.

19. The digital processing system of claim 17, wherein the first identifier includes "0s" and the second identifier includes "1s."

20. The digital processing system of claim 17, wherein the storage device is to store a client identification and a corresponding unique combination of watermarked copies for the client.

21. The digital processing system of claim 17, wherein the storage device is to store a neutral scrambled copy of the content.

22. The digital processing system of claim 21, wherein the processing unit is to combine at least one part of the neutral encrypted copy with parts of the encrypted copy watermarked with the first identifier and with parts of the encrypted copy watermarked with the second identifier.

23. A digital processing system comprising:

a receiving module to provide clear content having a plurality of double parts, a first part watermarked with a first identifier and a second part watermarked with a second identifier;

an encryption module coupled to the receiving module, the encryption module to encrypt the clear content with a first key, to encrypt the first part watermarked with the first identifier with a second key, and to encrypt the second part watermarked with the second identifier with a third key; and

a key management module to manage the keys as to allow one or more clients to decrypt the encrypted content with a combination of encrypted first and second parts

watermarked with the first identifier and second identifier, respectively, unique to each client.

24. The digital processing system of claim 23, wherein the first identifier includes "0s" and the second identifier includes "1s."

25. The digital processing system of claim 23, wherein the encryption module is to provide entitlement control messages (ECMs) using the first key, second key, and third key, wherein the second and third key are alternated to obtain a unique combinations of "0s" and "1s" unique to each client.

26. The digital processing system of claim 23, wherein the storage device is to store a client identification and a corresponding unique combination of watermarked copies for the client.

27. A computer-implemented method comprising:  
watermarking first and second copies of content with respective first and second watermarks;  
encrypting the first copy of content using a first and the second copy of the content using a second key; and  
combining encrypted copies into a single stream of data.

28. The computer-implemented method of claim 27, further comprising:  
multicasting the single stream of data to one or more clients.
29. The computer-implemented method of claim 27, further comprising:  
storing the unique keys and common key in a database, the database including an  
array matching the unique keys to the unique watermarks.
30. The computer-implemented method of claim 29, further comprising:  
selectively unicasting the unique keys to one or more clients.
31. The computer-implemented method of claim 30, further comprising:  
associating each client to the unique keys received and watermarks in the stream  
of data.
32. A server comprising:  
a storage device to store content;  
a processing unit to watermark redundant parts in the content with one or more  
unique watermarks, to encrypt the watermarked redundant parts using a unique key for  
each unique watermark and the remaining parts of the stream of content with a common  
key, and to combine the encrypted parts into a single stream of data.
33. The server of claim 32, wherein the processing unit is to multicast the single  
stream of data to one or more clients.

34. The server of claim 32, further comprising:

a database to store the unique keys and common key, the database including an array matching the unique keys to the unique watermarks.

35. The server of claim 32, wherein the processing unit is to unicast selectively the unique keys to one or more clients.

36. The server of claim 32, wherein the processing unit is to associate each client to the unique keys and watermarks in the stream of data.

37. A computing system comprising:

means for storing content;

means for watermarking redundant parts in the content with one or more unique watermarks;

means for encrypting the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key; and

means for combining the encrypted parts into a single stream of data.

38. The computing system of claim 37, further comprising:

means for multicasting the single stream of data to one or more clients.



39. The computing system of claim 37, further comprising:  
means for storing in a database the unique keys and common key, the database including an array matching the unique keys to the unique watermarks.
40. The computing system of claim 37, further comprising:  
means for unicasting selectively the unique keys to one or more clients.
41. The computing system of claim 37, further comprising:  
means for associating each client to the unique keys and watermarks in the stream of data.
42. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:  
watermarking redundant parts in content with one or more unique watermarks;  
encrypting the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key; and  
combining encrypted parts into a single stream of data.
42. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:  
watermarking redundant parts in content with one or more unique watermarks;  
encrypting the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key; and

combining encrypted parts into a single stream of data.

43. <sup>43</sup> A method of distributing content, the method comprising:

watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying both the first and second duplicates of the content portion to first and second users; and

supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

44. <sup>44</sup> The method of claim 43, wherein the content includes text, audio, or video content.

45. <sup>45</sup> The method of claim 43, wherein the supplying of the first and second duplicates and keys includes supplying the first and second duplicates and keys via a network.

46. <sup>46</sup> The method of claim 45, wherein the network includes an Internet network.

47. An apparatus comprising:

48 watermarking means for watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting means for encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying means for supplying both the first and second duplicates of the content portion to first and second users; and

supplying means for supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

49  
48. The apparatus of claim 47, wherein the content includes text, audio, or video content.

50  
49. The apparatus of claim 47, wherein the supplying means for the first and second duplicates and keys include supplying means for supplying the first and second duplicates and keys via a network.

51  
50. The apparatus of claim 49, wherein the network includes an Internet network.

51. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:

watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying both the first and second duplicates of the content portion to first and second users; and

supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

52. A method of distributing content, the method comprising:

watermarking multiple sets of duplicated content portions with multiple sets of identifiers, each identifier of each set being unique to a specific duplicated content portion;

encrypting each duplicated content portion within each set with a respective key of a plurality of keys;

supplying the multiple sets of duplicated content portions to multiple users; and

supplying a unique set of keys, selected from the plurality of keys, to each of the multiple users so that each of the multiple users is enabled to decrypt the multiple sets of

duplicated content portions to generate content embodying a unique sequence of  
 identifiers.

53. <sup>52</sup> The method of claim 52, wherein the supplying of the multiple sets of duplicated  
 content portions includes multicasting the multiple sets of duplicated content portions to  
 the multiple users on an Internet network.

54. <sup>53</sup> The method of claim 53, wherein the supplying of the unique sets of keys to each  
 of the multiple users includes unicasting the unique set of keys to each of the multiple  
 users on the Internet network.

55. <sup>54</sup> The method of claim 52, wherein the content portions include text, audio, or video  
 content portions.

56. <sup>55</sup> An apparatus comprising:  
     watermarking means for watermarking multiple sets of duplicated content  
 portions with multiple sets of identifiers, each identifier of each set being unique to a  
 specific duplicated content portion;  
     encrypting means for encrypting each duplicated content portion within each set  
 with a respective key of a plurality of keys;  
     supplying means for supplying the multiple sets of duplicated content portions to  
 multiple users; and

supplying means for supplying a unique set of keys, selected from the plurality of keys, to each of the multiple users so that each of the multiple users is enabled to decrypt the multiple sets of duplicated content portions to generate content embodying a unique sequence of identifiers.

58  
57. The apparatus of claim 56, wherein the supplying means for supplying of the multiple sets of duplicated content portions includes multicasting means for multicasting the multiple sets of duplicated content portions to the multiple users on an Internet network.

59  
58. The apparatus of claim 57, wherein the supplying means for supplying of the unique sets of keys to each of the multiple users includes unicasting means for unicasting the unique set of keys to each of the multiple users on the Internet network.

60  
59. The apparatus of claim 56, wherein the content portions include text, audio, or video content portions.

61  
60. A machine-readable medium providing instructions, which if executed by a processors, causes the processor to perform an operation comprising:

watermarking multiple sets of duplicated content portions with multiple sets of identifiers, each identifier of each set being unique to a specific duplicated content portion;

encrypting each duplicated content portion within each set with a respective key  
of a plurality of keys;

supplying the multiple sets of duplicated content portions to multiple users; and

supplying a unique set of keys, selected from the plurality of keys, to each of the  
multiple users so that each of the multiple users is enabled to decrypt the multiple sets of  
duplicated content portions to generate content embodying a unique sequence of  
identifiers.